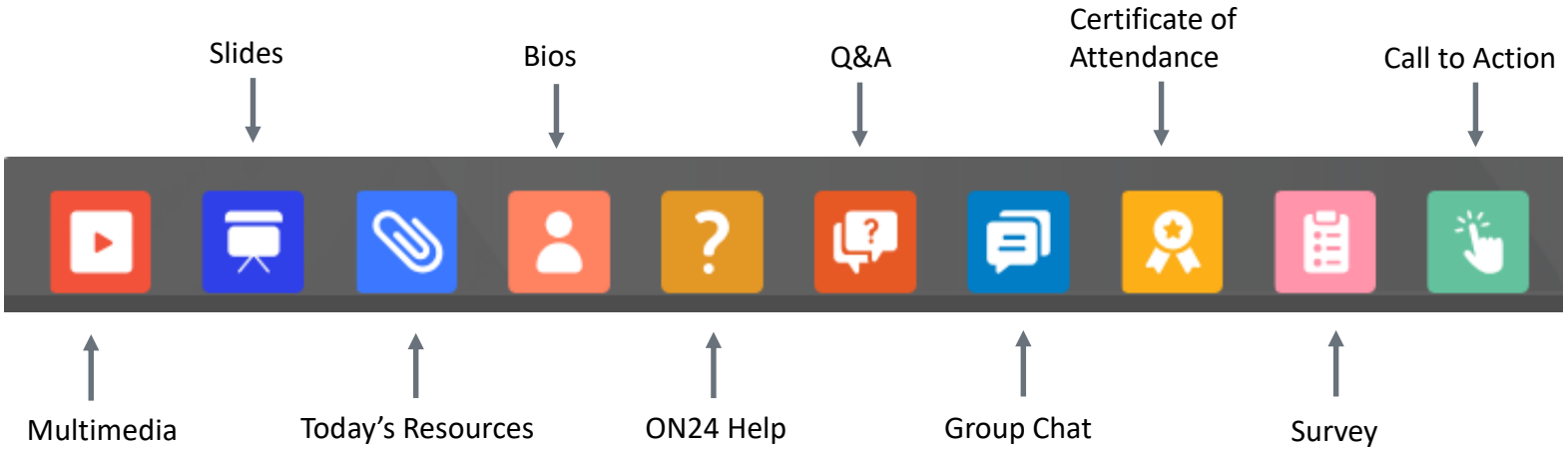

# CompTIA Network+ N10-009 TTT Session 6:

## Title

June 20, 2024

CompTIA

@TeachCompTIA #NetworkPlusTTT



# Network+ Team

Instructor:
Don Tilley
Cybersecurity Instructor,
Program Director
Access Computer Training
dontilley130@gmail.com

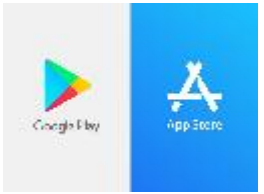
Host:
Stephen Schneiter
Instructor Network Program Director
CompTIA
sschneiter@comptia.org

CompTIA INSTRUCTOR NETWORK

The CompTIA Instructor Network (CIN) is a worldwide community for instructors who provide CompTIA certification training.

Benefits of being a community member include:

- Communicate and collaborate with CompTIA staff and other instructors.
- Access resources for students to understand the value of getting certified.
- Receive complimentary training and tools from CompTIA to enrich your classroom.
- Become proficient at teaching CompTIA standards.
- Share best practices and resources with each other.



https://cin.comptia.org

PARTNERSUMMIT 24

JULY 30TH

CompTIA INSTRUCTOR NETWORK

# TRAIN THE TRAINER

## WORKSHOPS

CompTIA Tech+

CompTIA Network+

CompTIA A+

Join us for the morning session from 9:00 a.m. to 12:00 p.m. or
the afternoon session from 1:00 p.m. to 4:00 p.m.
Each session is $99.00.
Lunch and refreshments provided

**Workshop sessions:**

1. Get In Sync with the new CompTIA Tech+ FC0-U71
2. Teaching CompTIA Network+ N10-009 with the new CertMaster Perform
3. Tools for teaching CompTIA A+ 1100 Series

**Each session provides:**

- Access to official CompTIA content for the course
- Instructor led training and labs
- Certificate of completion provided at the end of session.

Hyatt Regency Atlanta
July 31 – August 1
Register today: https://connect.comptia.org/partnersummit/home


If a bad organizational culture eats ethics for breakfast, then will AI steal your lunch money?

What: One-hour webinar investigating current industry AI trends
When: Thursday July 25th 10:00 a.m. CST
Where: ON24
Who: James Stanger, Chief Technology Evangelist
**Register: https://bit.ly/CINPulse-AITrends**

@TeachCompTIA

# Agenda

- Introductions
- Getting to know you
- Why Network+
- Session 1 topics

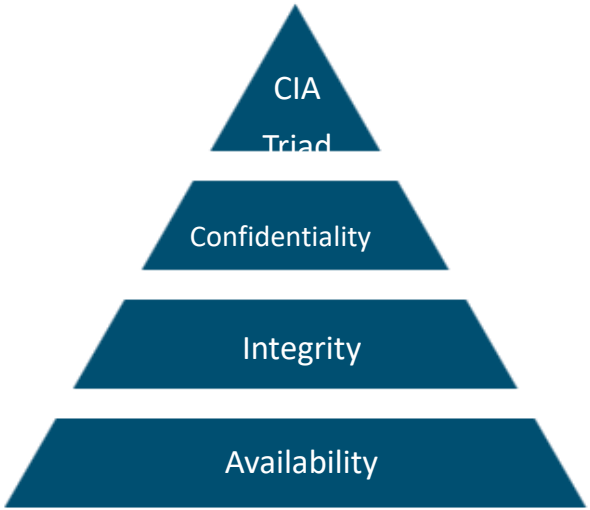
| Network+ N10-009 TTT Session Outline | |
|---|---|
| Date | Topic |
| ✓ 06/20/2024 | Introduction and Network Topologies |
| ✓ 06/25/2024 | Cabling and Physical Installations |
| ✓ 06/27/2024 | Configuring Interfaces and Switches |
| ✓ 07/02/2024 | Configuring Network Addressing |
| ✓ 07/09/2024 | Configuring Routing and Advanced Switching |
| ✓ 07/11/2024 | Network Security |
| 07/16/2024 | Network Security (Continued) |
| 07/18/2024 | Wireless Networking |
| 07/23/2024 | Troubleshooting and Management |
| 07/25/2024 | Emerging Technologies and Trends |

# Learning Objectives

- Explain common security concepts.
- Distinguish risk, vulnerability, exploit, and threat.
- Explain the importance of audits and regulatory compliance.
- Summarize types of attacks and their impact on the network.
- Explain identity and access management concepts.
- Distinguish protocols and standards used for authentication and directory management.

# SECURITY CONCEPTS

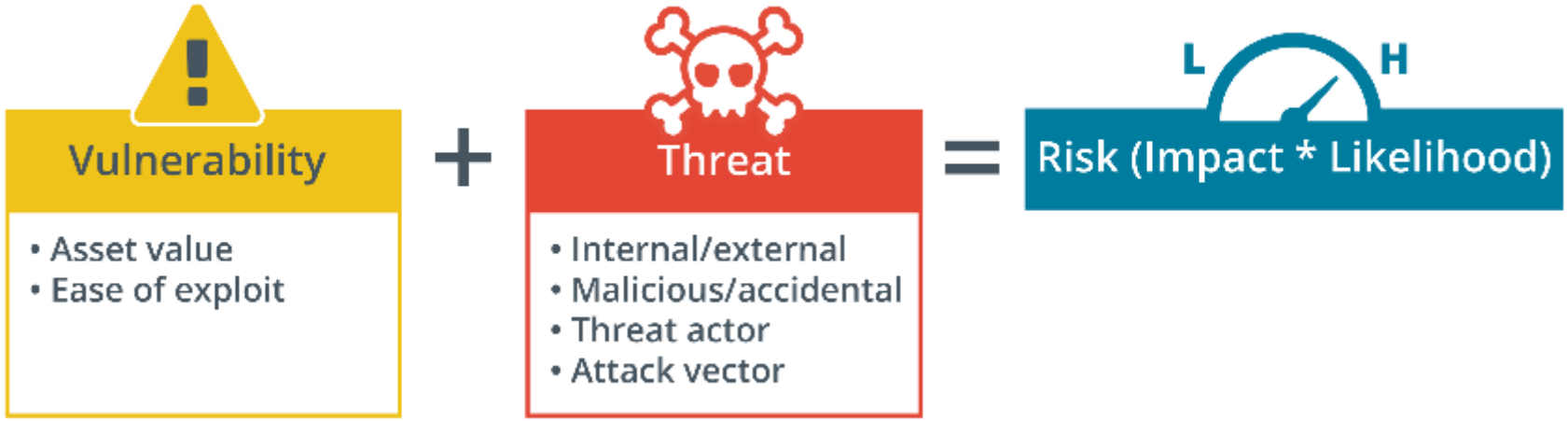
# CIA Triad






1
1

# Vulnerability, Threat, Risk



# Security Audits

## Security Audit

Systematic evaluation of a company's information system security

Measure conformity to established security criteria

Identifies strengths and weaknesses

Highlights areas for security improvement

## Key Components

Policies assessment

Procedures review

Technical controls evaluation

Access controls inspection

Risk management practices assessment

# Types of Security Assessments

**•Compliance Audits**

- Verify adherence to laws, regulations, and standards

**•Risk-Based Audits**

- Identifying and prioritizing potential threats/vulnerabilities

**•Technical Audits**

- Deep-dive into IT infrastructure (e.g., network security, access controls, and data protection)

# Role of Risk Management

**Identifying Critical Assets**

Determine mission essential functions/assets vital to business operations

**Business Impact Analysis (BIA)**

Assess potential losses from threat scenarios (e.g., DoS attack)

**Mitigation Strategies**

Balance cost of security controls against the potential risks to determine acceptable risk levels

# Regulatory Compliance

## Definition

The process by which organizations ensure they are following all relevant laws, regulations, and guidelines applicable to their industry

## Purpose

To protect data, individuals' privacy, and ensure the integrity of financial transactions and sensitive information

## Key Components

Implementation of security measures and controls

Regular internal and external audits

Compliance with specific industry standards

# Understanding Encryption

## What is Encryption?

Converting human-readable data (plaintext) into a coded format (ciphertext)

Only accessible to authorized users with decryption key

## Purpose of Encryption

Ensures data confidentiality

Protects information from unauthorized access

# Types of Cryptographic Algorithms

## Encryption Algorithm

Converts plaintext into ciphertext (key required for decryption)

Use Case: Protecting emails or files

## Cryptographic Hash Algorithm

Transforms a string into a fixed-length hash (cannot be reversed)

Use Case: Password storage, verifying data integrity

# The States of Data

## •Data at Rest

- Persistent storage media protection
- Example: encrypted hard drives

## •Data in Transit

- Protection while data is transmitted
- Example: TLS encryption

## •Data in Use

- Securing data in volatile memory
- Example: RAM encryption techniques

# Vulnerabilities

| 1.Definition | •Causes | •Impact | •Targets |
| --- | --- | --- | --- |
| • Flaws in software design allowing bypass of security or causing crashes | • Misconfigurations, poor practices, design faults | • Allows attackers to execute arbitrary code, install malware, compromise security configurations | • Commonly include web servers, browsers, plug-ins, email clients, databases |

# Types of Exploits and Vulnerabilities

## 1.Zero-Day Vulnerabilities

- Exploited before developers can patch
- High destructive potential

## •Unpatched/Legacy Systems

- Pose significant threats due to lack of updates or support

## •Vulnerability Assessment

- Evaluating a system's security based on its configuration
- Verify it matches the ideal baseline
- Involves manual inspections and automated scans

Question 1: What are the three components of the CIA Triad?

Question 2: What is the difference between a vulnerability and a threat in cybersecurity?

# NETWORK THREATS AND ATTACKS

# External Threats

- **Origin**
  - Attacks or malicious activities by individuals/ groups from outside the organization
- **Examples**
  - Hackers
  - Cyber Criminals
  - Espionage
  - Competitive intelligence

- **Characteristics**
  - Often sophisticated
  - Targeted
  - Relentless
- **Mitigation Strategies**
  - Firewall protection
  - Intrusion detection systems (IDS)
  - External audits
  - Security awareness training

# Internal Threats

- Origin
  - Originate from within the organization
  - Often involve employees, contractors, or business partners
- Examples
  - Accidental data leaks
  - Deliberate data theft
  - Sabotage
  - Insider trading

- Characteristics
  - Harder to detect due to legitimate access
  - May stem from dissatisfaction, malicious intent, or carelessness
- Mitigation Strategies
  - Role-based access controls
  - User activity monitoring
  - Regular security training
  - Clear policies on data handling

# Denial of Service (DOS) Attacks

## Origin

Internet's inception and growing more complex

Evolved to sophisticated DDoS using botnets

## Characteristics

Intent: Disrupts service, denying user access.

Methods: Uses resource exhaustion, bandwidth saturation, software exploitation

Impact: Service degradation to complete shutdown

# DDoS Attacks – Examples and Mitigation

## Examples of DDoS Attacks

ICMP Flood: Overloads with ICMP packets (unreachable targets)

SYN Flood: Abuses TCP handshake (blocks legitimate server access)

DNS Amplification: Exploits misconfigured DNS servers (attack traffic)

## Mitigation Strategies

Early Detection: Monitors for unusual traffic patterns

Traffic Filtering: Employs firewalls and IDS to block malicious traffic

Response Plan: Prepares specific actions for DoS attacks

Redundancy: Implements network redundancy to reduce downtime

# Botnet Attacks

## Definition

Network of compromised computers for malicious use

Infected by malware and controlled remotely

## Types of Botnets

Distributed Denial of Service (DDoS)

Spam botnets

Banking trojan botnets

## Mitigation strategies

- Implement cybersecurity like firewalls and antivirus
- Analyze network for unusual traffic
- Isolate and fix compromised devices
- Teach safe internet use

# Malware

## Definition

Harmful software disrupting or damaging systems

## Types of Malware

Viruses/Worms

Trojan

PUPs/PUAs

## Vectors and Payloads

Vectors: Infection and spread methods

Payloads: Executed harmful actions (e.g., spying, unauthorized access, data encryption for ransom)

Question 1: What is the main difference between external and internal threats?

Question 2: What is a Denial of Service (DoS) attack?

# SPOOFING ATTACKS

# Spoofing Attacks

| Definition | Purpose | Types |
| --- | --- | --- |
| Disguising oneself as someone else to gain unauthorized access | Trick users/devices, bypass security, and steal data or spread malware | IP spoofing<br>ARP spoofing<br>Email spoofing |

# On-Path Attacks

## Definition

Attacks that intercept and possibly alter two parties' communications undetected

## Purpose

Steal sensitive personal or corporate information

Inject malware

## Common Types

Session hijacking

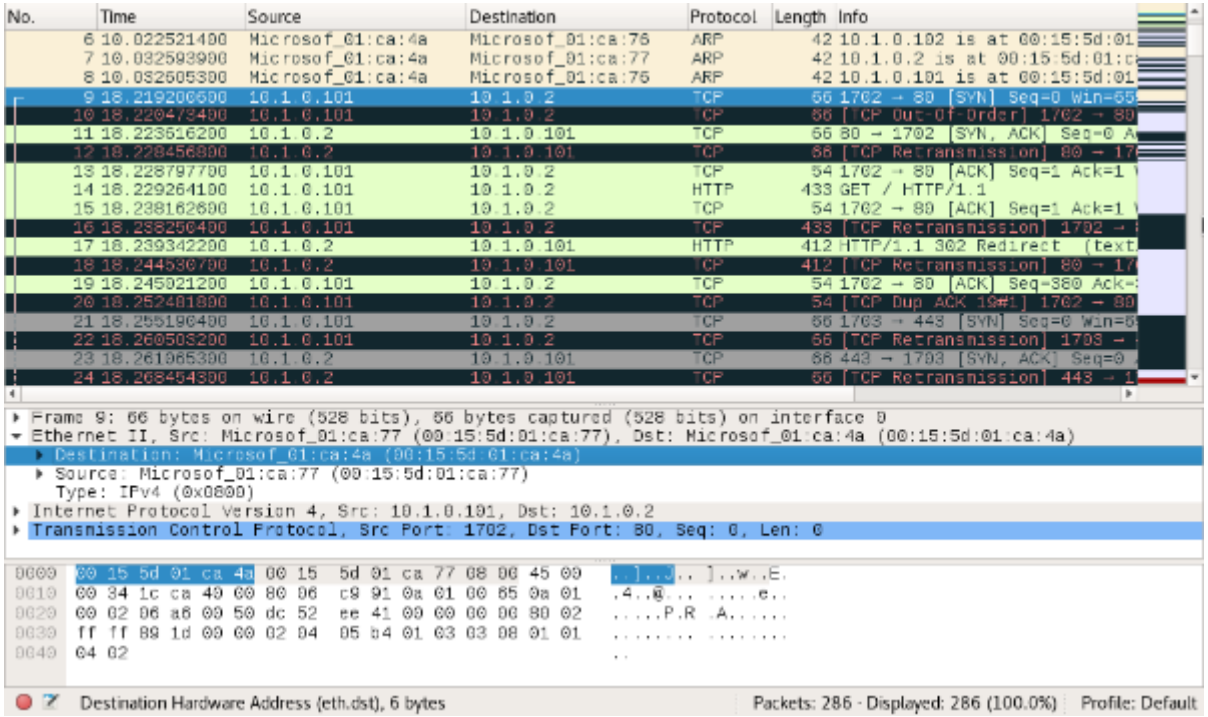
SSL stripping

DNS spoofing

Wi-Fi eavesdropping

ARP spoofing

# ARP Spoofing Example



# MAC Flooding Attacks

## Definition

Overloads switch CAM table with many MAC addresses, causing switch failure and traffic broadcast

## Purpose

Disrupt switch function to eavesdrop on normally inaccessible network traffic

## Types of MAC Flooding Attacks

Random MAC address flooding

Incremental MAC address flooding

Targeted MAC flooding

# VLAN Hopping Attack

| •Definition | •Purpose | •Types |
| --- | --- | --- |
| • Exploit where attackers send packets to a VLAN without access, using vulnerabilities in VLAN implementation on switches | • Bypass security, accessing restricted/sensitive networks | • Switch Spoofing<br>• Double Tagging |

# Activity: Fill in the Blank

Two types of _____ hopping attacks include switch spoofing and double tagging.

A/an _____ attack involves intercepting and possibly altering two parties' communications without detection.

A/an _____ flooding attack overloads switch CAM table with many addresses, causing switch failure and traffic broadcast

# ROGUE SYSTEM ATTACKS

# Rogue Devices and Services

## Definition

Unauthorized hardware and software that connect to a network without permission, potentially causing serious security risks

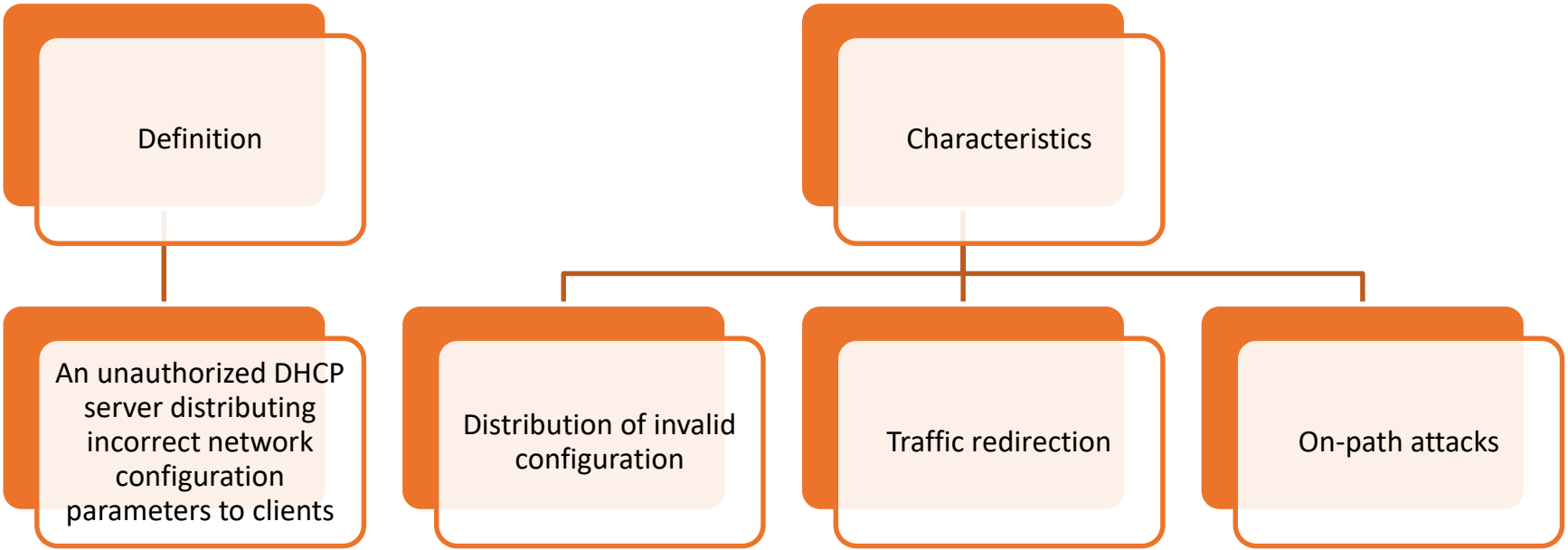
## Characteristics

Unauthorized access

Malicious intent

Data interceptions and manipulation

# Rogue DHCP Server Attacks



# DNS Attacks

## Definition

Attacks that target the DNS, undermining the integrity and availability of internet services

## Characteristics

Disruption of service

Domain hijacking

Cache poisoning

Question 1: What is a rogue DHCP server attack?

Question 2: What are some characteristics of rogue devices and services?

# SOCIAL ENGINEERING

# Social Engineering Attacks

## Definition

Manipulative technique cyber criminals use to exploit human vulnerabilities, not technical weaknesses

## Goal

Deceive individuals into giving up confidential or personal information

## Characteristics

Highly effective due to exploiting people's natural tendency to trust

Success relies on the attacker appearing trustworthy or authoritative

Persuades victims to breach security practices or ignore red flags

# Types of Social Engineering Attacks

Shoulder Surfing

Dumpster Diving

Tailgating/Piggybacking

Phishing

# Password Attacks

## Definition

Attempts to obtain or bypass individuals' passwords using various methods

## Dictionary Attacks

Enters all dictionary words

Targets weak, simple passwords

## Brute Force Attacks

Tries all character combinations

Time-consuming but cracks any password

Question 1: What is the primary goal of social engineering attacks?

Question 2: Name two types of social engineering attacks.

# AUTHENTICATION

# Discussion

## Boarding Pass

Passenger Name: Samantha Simons
Birthdate: 1-11-2001

Required to board:

- Passport
- Printed Ticket

Destination: Aruba
Ship: The Splash
Deck: 12
Cabin: 12345

Included:

- ✓ Beverages: All-inclusive
- ✓ Meals: A la carte
- ✓ Scuba diving excursion
- ✓ Resort shopping excursion

*All onboard activities and purchases will be logged in your customer account.*

**Identity**
Who she claims to be

**Authentication**
Proof that she is who she claims to be

**Authorization**
Where she is allowed to go and what level of access she will have once onboard

**Accounting**
Method for tracking and logging activity

# Think About It: Access Control

| | |
|---|---|
| **Identity** | An account or ID that uniquely represents a user, device, or process on the network |
| **Authentication** | Factor(s) used to prove a subject is who or what it claims to be |
| **Authorization** | Rights and permissions a subject is granted within a system or network |
| **Accounting** | Tracking of authorized/unauthorized usage of a resource by a subject |

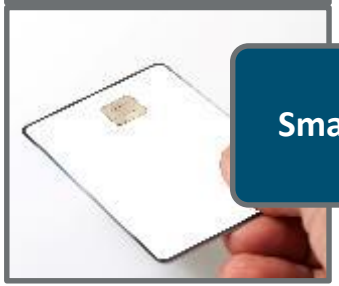
What are some examples of each of these in network security?

# Authentication Methods

**Something you know**

Password

**Something you have**

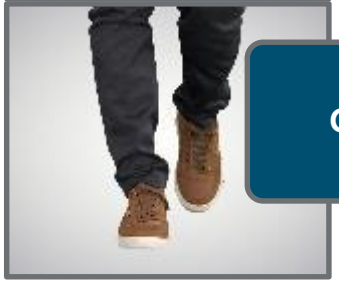


Smart card

**Something you are**

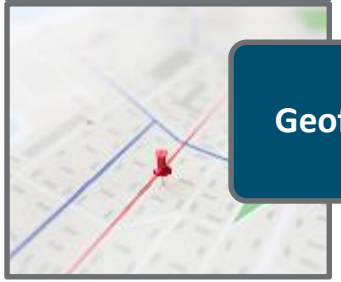
Fingerprint

**Something you do**



Gait

**Somewhere you are**

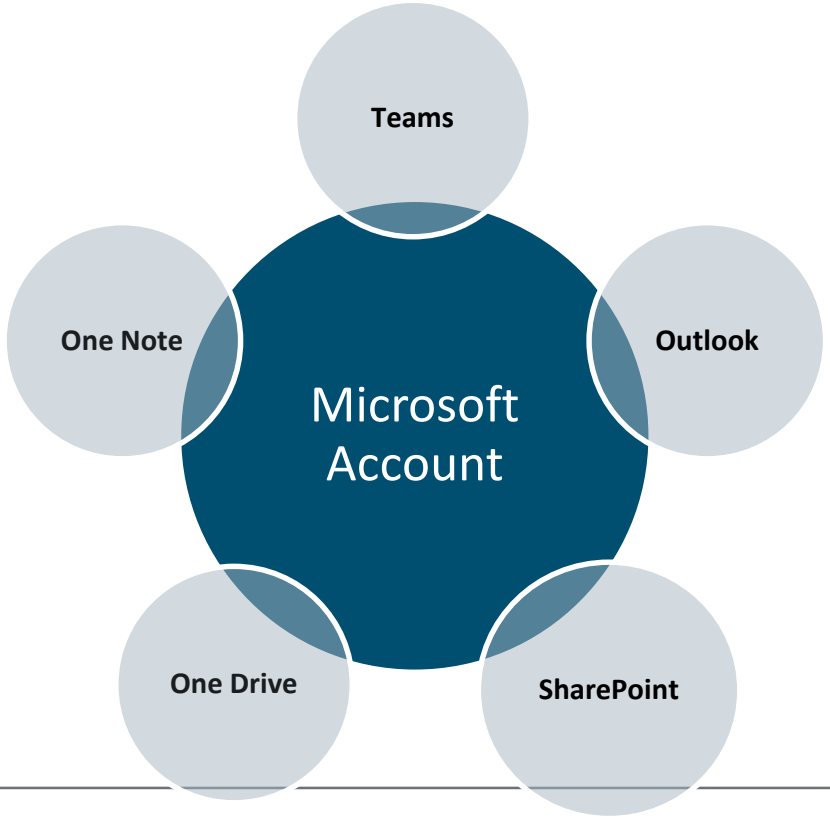


Geofencing

**Somewhen you are**

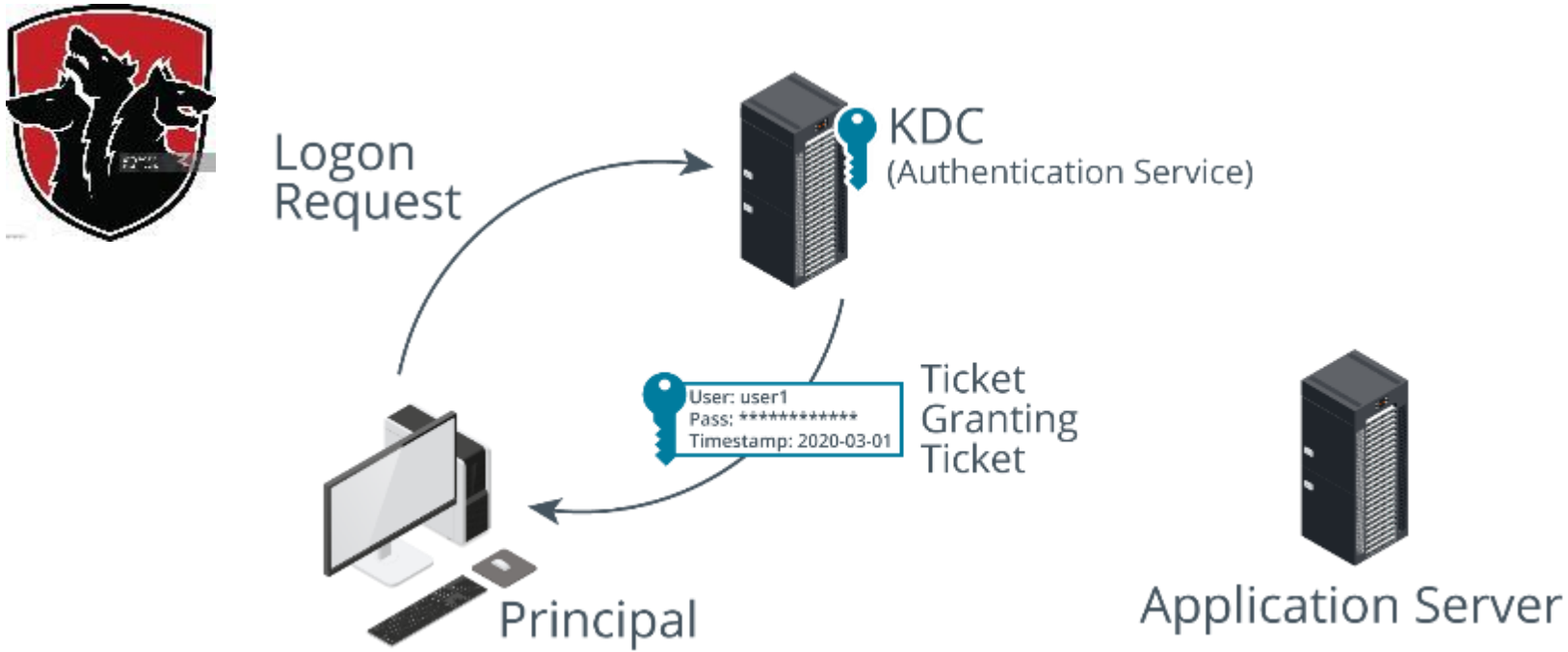
Time restrictions

# Single Sign-On




I’m so happy I don’t have to log in to all these apps one at a time!

# Kerberos SSO Authentication



Question 1: What are the three main factors of authentication often referred to as "something you..."?

Question 2: What is Single Sign-On (SSO) and how does it benefit users?

Question 3: What is the primary function of the Ticket Granting Service (TGS) in Kerberos authentication?

Question 4: What are two key benefits of using Kerberos for authentication?

# Summary

**Policies & Controls**: Establish policies and deploy controls aligned with the CIA triad (Confidentiality, Integrity, Availability)

**Assessment & Monitoring**: Use tools and processes to continuously evaluate vulnerabilities, threats, and risk

**Awareness Training**: Educate users on common attacks like footprinting, spoofing, DoS, DNS manipulation, VLAN hopping, malware, password cracking, and social engineering

**Access control**: Only authorized users and devices can access resources (physical & digital measures).

# Chat Question

Discussion question asked to the group.

Answer in the chat window and let’s share.

# Discussion time: Please type your questions in chat

- Questions over content.
- Share you experience.
- What would you like to see different moving forward?


Let’s keep the conversation going in the CompTIA Instructor Forum: https://cin.comptia.org